Complementarity in Quantum Systems

Dénes Petz [1]

Alfréd Rényi Institute of Mathematics
Hungarian Academy of Sciences
H-1053 Budapest, Reáltanoda u. 13-15, Hungary

Abstract: Reduction of a state of a quantum system to a subsystem gives partial quantum information about the true state of the total system. Two subalgebras $\mathcal{A}_1$ and $\mathcal{A}_2$ of $B(\mathcal{H})$ are called complementary if the traceless subspaces of $\mathcal{A}_1$ and $\mathcal{A}_2$ are orthogonal (with respect to the Hilbert-Schmidt inner product). When both subalgebras are maximal Abelian, then the concept reduces to complementary observables or mutually unbiased bases. In the paper several characterizations of complementary subalgebras are given in the general case and several examples are presented. For a 4-level quantum system, the structure of complementary subalgebras can be described very well, the Cartan decomposition of unitaries plays a role. It turns out that a measurement corresponding to the Bell basis is complementary to any local measurement of the two-qubit-system.

Key words: Entropic uncertainty relation, mutually unbiased basis, CAR algebra, commuting squares, complementarity, Cartan decomposition, Bell states.

The study of complementary observables goes back to early quantum mechanics. Position and momentum are the typical examples of complementary observables and the main subject was the joint measurement and the uncertainty [8, 9]. In the setting of finite dimensional Hilbert space and in a mathematically rigorous approach, the paper [24] of Schwinger might have been the first in 1960. The goal of that paper is the finite dimensional approximation of the canonical commutation relation. An observable of a finite system can be identified with a basis of the Hilbert space through the spectral theorem [1] and instead of complementarity the expression "mutually unbiased" became popular [28]. The maximum number of mutually unbiased bases is still and open question [22], nevertheless such bases are used in several contexts, state determination, the "Mean King's problem", quantum cryptography etc. [12, 13, 6].

[1]E-mail: petz@math.bme.hu. Partially supported by the Hungarian Research Grant OTKA T032662.

Motivated by the frequent use of mutually unbiased bases and complementary reductions of two qubits [19, 21], the goal of this paper is a general study of complementary subalgebras. The particular case, when the subalgebras are maximal Abelian, corresponds to complementary observables, or mutually unbiased bases. This case has been studied in the literature by many people. If the reduction of a quantum state to a subalgebra is known to us, then this means a partial information about the state. The concept of complementarity of two subsystems means heuristically that the partial information provided jointly by the two subsystems is the largest when it is compared with the information content of the two subsystems [28].

The paper is organized in the following way. First the entropic uncertainty relation of Maasen and Uffink is reviewed as a motivation for the concept of complementarity (of observables or basis). Then the complementarity of observables is reformulated in terms of commutative subalgebras. This reformulation leads to the complementarity of more general subalgebras (corresponding to a subsystem of a quantum system). It turns out that complementarity is a common generalization of the ordinary tensor product and the twisted fermionic tensor product. When two subalgebras are unitarily equivalent, complementarity can be read out from the unitary when it is viewed as a block-matrix. A modification of the construction of complementary bases (going back to Schwinger) yields examples of complementary subalgebras in arbitrary dimension. The maximal number of complementary subalgebras remains an open question, however, the case of 4-level quantum system is analyzed in details. It turns out that a measurement corresponding to the Bell basis is complementary to any local measurement of the two-qubit-system.

1 Complementary observables

Let A and B be two self-adjoint operators on a finite dimensional Hilbert space. If $A = \sum_i \lambda_i^A P_i^A$ and $B = \sum_i \lambda_i^B P_i^B$ are their spectral decompositions, then

$$H(A, \varphi) = \sum_i \eta(\varphi(P_i^A)) \quad \text{and} \quad H(B, \varphi) = \sum_i \eta(\varphi(P_i^B))$$

are the **entropies** of A and B in a state φ. ($\eta(t)$ is the function $-t \log t$.)

Assume that the eigenvalues of A and B are free from multiplicities. If these observables share a common eigenvector and the system is prepared in the corresponding state, then the measurement of both A and B leads to a sharp distribution and one cannot speak of uncertainty. In order to exclude this case, let (e_i) be an orthonormal basis consisting of eigenvectors of A, let (f_i) be a similar basis for B and we suppose that

$$c^2 := \sup \{ |\langle e_i, f_j \rangle|^2 \colon i, j \} \tag{1}$$

is strictly smaller than 1. Then $H(A, \varphi) + H(B, \varphi) > 0$ for every pure state φ. Since the left-hand-side is concave in φ, it follows that $H(A, \varphi) + H(B, \varphi) > 0$ for any state

φ. This inequality is a sort of uncertainty relation. The lower bound was conjectured in [14] and proven by Maasen and Uffink in [16].

Theorem 1 *With the notation above the uncertainty relation*

$$H(A,\varphi)+H(B,\varphi)\ge -2\log c$$

holds.

Let n be the dimension of the underlying Hilbert space. We may assume that φ is a pure state corresponding to a vector Φ. Then $\varphi(P_i^A)=|\langle e_i,\Phi\rangle|^2$ and $\varphi(P_i^B)=|\langle f_i,\Phi\rangle|^2$.

The $n\times n$ matrix $T_{i,j}:=(\langle e_i,f_j\rangle)_{i,j}$ is unitary and T sends the vector

$$f:=(\langle e_1,\Phi\rangle,\langle e_2,\Phi\rangle,\dots,\langle e_n,\Phi\rangle)$$

into

$$Tf=(\langle f_1,\Phi\rangle,\langle f_2,\Phi\rangle,\dots,\langle f_n,\Phi\rangle)\,.$$

The vectors f and Tf are elements of $\mathbb{C}^n$ and this space may be endowed with different L^p norms. Using interpolation theory we shall estimate the norm of the linear transformation T with respect to different L^p norms. Since T is a unitary

$$\|g\|_2=\|Tg\|_2 \qquad (g\in\mathbb{C}^n)\,.$$

With the notation (1) we have also

$$\|Tg\|_\infty\le c\|g\|_1 \qquad (g\in\mathbb{C}^n)\,.$$

Let us set

$$N(p,p')=\sup\{\|Tg\|_p/\|g\|_{p'}\colon g\in\mathbb{C}^n,\quad g\neq 0\}$$

for $1\le p\le\infty$ and $1\le p'\le\infty$. The **Riesz–Thorin convexity theorem** says that the function

$$(t,s)\mapsto \log N(t^{-1},s^{-1}) \tag{2}$$

is convex on $[0,1]\times[0,1]$ (where 0^{-1} is understood to be ∞). Application of convexity of (2) on the segment $[(0,1),(1/2,1/2)]$ yields

$$\|Tg\|_{2/\lambda}\le c^{1-\lambda}\|g\|_\mu \qquad (g\in\mathbb{C}^n)\,,$$

where $0<\lambda<1$ and $\mu=(1-\lambda/2)^{-1}$. This is rewritten by means of a more convenient parameterization in the form

$$\|Tg\|_p\le c^{1-2/p}\|g\|_q \qquad (g\in\mathbb{C}^n)\,,$$

where $2\le p<\infty$ and $p^{-1}+q^{-1}=1$. Consequently

$$\log\|Tf\|_p\le\left(1-\frac{2}{p}\right)\log c+\log\|f\|_q\,. \tag{3}$$

One checks easily that

$$\frac{d\log\|Tf\|_p}{dp}\Big|_{p=2}=-\frac{1}{4}H(B,\varphi)\quad\text{and}\quad\frac{d\log\|f\|_q}{dp}\Big|_{p=2}=\frac{1}{4}H(A,\varphi)\,.$$

Hence dividing (3) by $p-2$ and letting $p\searrow 2$ we obtain

$$-\tfrac{1}{4}H(B,\varphi)\le\tfrac{1}{2}\log c+\tfrac{1}{4}H(A,\varphi)$$

which proves the theorem for a pure state.

Concavity of the left hand side of the stated inequality in φ ensures the lower estimate for mixed states. □

The theorem can be formulated in an algebraic language. Let $\mathcal{A}$ and $\mathcal{B}$ be maximal Abelian subalgebras of the algebra $M_n(\mathbb{C})$ of $n\times n$ matrices. Set

$$c^2:=\sup\{\mathrm{Tr}\,PQ: P\in\mathcal{A}, Q\in\mathcal{B}\text{ are minimal projections}\}. \tag{4}$$

The theorem tells that

$$H(\varphi|\mathcal{A})+H(\varphi|\mathcal{B})\ge -2\log c\,. \tag{5}$$

Both the definition of c and the statement are formulated without the underlying Hilbert space.

Question 1 Can we make the proof of (5) without using the Hilbert space?

Let A and B self-adjoint operators with eigenvectors (e_j) and (f_i), respectively and let φ be the pure state corresponding to e_1. Then $H(A,\varphi)=0$ and $H(B,\varphi)=\log n$. Hence this example shows that the lower bound for the entropy sum in Theorem 1 is sharp. If (6) holds then the pair (A,B) of observables are called **complementary** [1]. According to another terminology, the bases $(e_j)_j$ and $(f_k)_k$ are called **mutually unbiased** if (6) holds. Mutually unbiased bases appeared in a different setting in the paper [12, 28], where state determination was discussed.

The lower bound in the uncertainty (5) is the largest if c^2 is the smallest. Since $n^2c^2\ge n$, the smallest value of c^2 is $1/n$. This happens if and only if

$$|\langle e_j,f_k\rangle|^2=n^{-1}\qquad (j,k=1,2,\dots,n)\,, \tag{6}$$

that is, the two bases are mutually unbiased. This is an extremal property of the mutually unbiased bases. The largest lower bound is attained if ϕ is a vector state generated by one of the basis vectors.

The complementarity of observables is also the property of the spectral measures associated with them. Therefore the extension to POVM's is natural. For a POVM $\mathcal{E}\equiv(E_i)_i$ and for a unit vector Φ, we define an entropy quantity as

$$H(\mathcal{E},\Phi)=\sum_i \mathrm{Tr}\,\eta(\langle\Phi,E_i\Phi\rangle).$$

Let $\mathcal{E} = (E_i)_i$ and $\mathcal{F} = (F_j)_j$ be POVM's on a Hilbert space $\mathcal{H}$ and $\Phi \in \mathcal{H}$ be a unit vector. Then the inequality

$$H(\mathcal{E}, \Phi) + H(\mathcal{F}, \Phi) \geq -2 \log \sup \left\{ \frac{|\langle \Phi, E_i F_j \Phi \rangle|}{\langle \Phi, E_i \Phi \rangle \langle \Phi, F_j \Phi \rangle} : i, j \right\}$$

holds and was proven in [15]. This estimate is essentially different from the uncertainty relation of Theorem 1. The lower bound here depends on the vector Φ.

Question 2 What is the lower bound if $F_j \Phi = \Phi$ for a certain j?

The uncertainty relation in Theorem 1 is for two observables. Assume that $n+1$ pairwise unbiased observables $A_1, A_2, \dots, A_{n+1}$ are measured when the system is in state φ. Sanchez [23] proved that

$$\sum_{k=1}^{n+1} H(A_k, \varphi) \geq (n+1) \log \frac{1}{2}(n+1). \tag{7}$$

2 Complementary subalgebras

There is an obvious correspondence between bases and maximal Abelian subalgebras. Given a basis, the linear operators diagonal in this basis form a maximal Abelian subalgebra, conversely if $|e_i\rangle\langle e_i|$ are minimal projections in a maximal Abelian subalgebra, then $(|e_i\rangle)_i$ is a basis. Parthasarathy characterized mutually unbiased bases through the corresponding maximal Abelian subalgebras.

Theorem 2 *Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be maximal Abelian subalgebras of $M_n(\mathbb{C})$. Then the following conditions are equivalent:*

(i) If $P \in \mathcal{A}_1$ and $Q \in \mathcal{A}_2$ are minimal projections, then $\mathrm{Tr}\, PQ = 1/n$.

(ii) The subspaces $\mathcal{A}_1 \ominus \mathbb{C}I$ and $\mathcal{A}_2 \ominus \mathbb{C}I$ are orthogonal in $M_n(\mathbb{C})$.

Mutually unbiased bases are interesting from many point of view [14, 4] and the maximal number of such bases is not completely known [26].

Subalgebras cannot be orthogonal. We say that the subalgebras $\mathcal{A}_1$ and $\mathcal{A}_2$ are **quasi-orthogonal** if $\mathcal{A}_1 \ominus \mathbb{C}I$ and $\mathcal{A}_2 \ominus \mathbb{C}I$ are orthogonal. If $\mathcal{A}_1$ and $\mathcal{A}_2$ are quasi-orthogonal, then we use the notation $\mathcal{A}_1 \perp_0 \mathcal{A}_2$. This terminology is mathematically very natural. However, from the view point of quantum mechanics, **complementarity** could be a better expression. If the subalgebras are maximal Abelian, then they correspond to observables and quasi-orthogonality of the subalgebras is equivalent to complementarity of the observables [1, 14, 17].

We consider subalgebras of $\mathcal{A} \equiv M_n(\mathbb{C})$ such that their minimal projections have the same trace. Such subalgebras will be called **homogeneous**. A maximal Abelian subalgebra and a subalgebra isomorphic to a full matrix algebra are homogeneous. (Recall that if $M_r(\mathbb{C}) \simeq \mathcal{A}_0 \subset M_n(\mathbb{C})$, then up to isomorphism $M_n(\mathbb{C}) = \mathcal{A}_0 \otimes M_s(\mathbb{C})$ and $rs = n$.)

The Hilbert-Schmidt inner product will be used in the form

$$\langle A, B \rangle = \tau(A^* B)\,, \tag{8}$$

where τ is the normalized trace. (Of course, orthogonality does not depend on the normalization of the trace.)

The next statement is an extension of Parthasarathy's result.

Theorem 3 *Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be homogeneous subalgebras of $M_n(\mathbb{C})$. Then the following conditions are equivalent:*

(i) If $P \in \mathcal{A}_1$ and $Q \in \mathcal{A}_2$ are minimal projections, then $\tau(PQ) = \tau(P)\tau)Q)$.

(ii) The subalgebras $\mathcal{A}_1$ and $\mathcal{A}_2$ are quasi-orthogonal in $M_n(\mathbb{C})$.

(iii) $\tau(A_1 A_2) = \tau(A_1)\tau(A_2)$ if $A_1 \in \mathcal{A}_1$, $A_2 \in \mathcal{A}_2$.

(iv) If $E_1 : \mathcal{A} \to \mathcal{A}_1$ is the trace preserving conditional expectation, then E_1 restricted to $\mathcal{A}_2$ is a linear functional (times I).

Proof: Note that $\tau((A_1 - I\tau(A_1))(A_2 - I\tau(A_2))) = 0$ and $\tau(A_1 A_2)) = \tau(A_1)\tau(A_2)$ are equivalent. If they hold for minimal projections, they hold for arbitrary operators as well. Moreover, (iv) is equivalent to the property $\tau(A_1 E_1(A_2)) = \tau(A_1(\tau(A_2))I)$ for every $A_1 \in \mathcal{A}_1$ and $A_2 \in \mathcal{A}_2$. $\square$

Condition (iii) is the independence of the subalgebras with respect to the tracial state. (Property (iii) is much weaker than the statistical independence of subalgebras, cf. [11].) Condition (iv) can be formulated as the following commuting square:

$$\begin{tikzcd}
& M_n(\mathbb{C}) \arrow[dl, "E_1"'] & \\
\mathcal{A}_1 & & \mathcal{A}_2 \arrow[ul] \arrow[dl, "\tau"] \\
& \mathbb{C}I \arrow[ul] &
\end{tikzcd}$$

Figure 1: Commuting square, $E_1|\mathcal{A}_2 = \tau(\,\cdot\,)I$.

Assume that $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_m$ are complementary maximal Abelian subalgebras of $M_n(\mathbb{C})$. Since the dimension of $\mathcal{A}_a \ominus \mathbb{C}I$ is $n-1$, the inequality $n^2 - 1 \geq m(n-1)$ holds. This implies that $m \leq n+1$.

3 Mutually unbiased bases

Let $\mathcal{H}$ be an n-dimensional Hilbert space. The standard construction of mutually unbiased bases goes through unitary operators. Assume that $U_0 \equiv I, U_1, \dots, U_{n^2-1}$ is a family of unitaries such that

$$\mathrm{Tr}\, U_j^* U_k = 0 \quad \text{for} j \neq k.$$

(In other words, $n^{-1/2} U_i$ is an orthonormal basis in $B(\mathcal{H})$, $0 \le i \le n^2 - 1$.)

Example 1 Let $e_0, e_1, \dots, e_{n-1}$ be a basis and let X be the unitary operator permuting the basis vectors cyclically:

$$Xe_i = \begin{cases} e_{i+1} & \text{if } 0 \le i \le n-2, \\ e_0 & \text{if } i = n-1. \end{cases}$$

Let $q := e^{\mathrm{i}2\pi/n}$ and define another unitary by $Ye_i = q^i e_i$. It is easy to check that $YX = qXY$ or more generally the commutation relation

$$Z^k X^\ell = q^{k\ell} X^\ell Z^k \tag{9}$$

is satisfied. For $S_{j,k} = Z^j X^k$, we have

$$S_{j,k} = \sum_{m=0}^{n-1} q^{mj} |e_m\rangle\langle e_{m+k}| \quad \text{and} \quad S_{j,k} S_{u,v} = q^{ku} S_{j+u,k+v},$$

where the additions $m+k, j+u, k+v$ are understood modulo n. (What we have is a finite analogue of the Weyl commutation relation, see [24].) Since $\mathrm{Tr}\, S_{j,k} = 0$ when at least one of j and k is not zero, the unitaries

$$\{S_{j,k} \,:\, 0 \le j, k \le n-1\}$$

are pairwise orthogonal.

Note that $S_{j,k}$ and $S_{u,v}$ commute if $ku = jv \mod n$.

In the case of $n = 2$, $X = \sigma_1$ and $Z = \sigma_3$. (This fact motivated our notation.) $\square$

Assume that $\mathcal{U}_1, \mathcal{U}_2, \dots, \mathcal{U}_{n+1}$ is a partition of the set $\{U_1, U_2, \dots, U_{n^2-1}\}$ such that $\#(\mathcal{U}_j) = n - 1$ and $\mathcal{U}_j$ consists of commuting unitaries. Then the maximal Abelian subalgebras $\mathcal{A}_i$ generated by $\mathcal{U}_i$ are pairwise complementary. (Note that $\mathcal{A}_i$ is the linear span of I and $\mathcal{U}_i$.) The remaining question is about the construction of the partition satisfying the requirements.

Example 2 Consider a 4-level quantum system and view $B(\mathcal{H})$ as $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$. The unitaries $\sigma_i \otimes \sigma_j$ form a basis and the partition

$$\sigma_0 \otimes \sigma_0,$$

$$\begin{gathered}\sigma_0 \otimes \sigma_1, \sigma_1 \otimes \sigma_0, \sigma_1 \otimes \sigma_1,\\ \sigma_0 \otimes \sigma_2, \sigma_2 \otimes \sigma_0, \sigma_2 \otimes \sigma_2,\\ \sigma_0 \otimes \sigma_3, \sigma_3 \otimes \sigma_0, \sigma_3 \otimes \sigma_3,\\ \sigma_1 \otimes \sigma_2, \sigma_2 \otimes \sigma_3, \sigma_3 \otimes \sigma_1,\\ \sigma_1 \otimes \sigma_3, \sigma_2 \otimes \sigma_1, \sigma_3 \otimes \sigma_2,\end{gathered}$$

determines 5 mutually unbiased bases.

The terminology of "*mutually unbiased bases*" was introduced in [28], where it was showed that the corresponding measurements "*provide an optimal means of determining an ensemble's state*". A slightly different extremal property of mutually unbiased bases is discussed in [20].

4 More about complementary subalgebras

If the pairwise complementary subalgebras $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_r$ are given and they span the whole algebra $\mathcal{A}$, then any operator is the sum of the components in the subspaces $\mathcal{A}_a \ominus \mathbb{C}I$ $(1 \le a \le r)$ and $\mathbb{C}I$:

$$A = -\tau(A)(r-1)I + \sum_{i=1}^{r} E_i(A)\,, \tag{10}$$

where $E_i : \mathcal{A} \to \mathcal{A}_i$ is the trace preserving conditional expectation (which is nothing else but the orthogonal projection with respect to the Hilbert-Schmidt inner product).

Example 3 Let $\mathcal{A}_1$ be the subalgebra $\mathbb{C}I \otimes M_r(\mathbb{C})$ and $\mathcal{A}_2$ be the subalgebra $M_p(\mathbb{C}) \otimes \mathbb{C}I$ of $M_p(\mathbb{C}) \otimes M_r(\mathbb{C})$. Then $\mathcal{A}_1$ and $\mathcal{A}_2$ are complementary.

For $p = r = 2$ we have

$$\mathcal{A}_1 = \left\{ \begin{bmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{bmatrix} : a, b, c, d \in \mathbb{C} \right\}, \quad \mathcal{A}_2 = \left\{ \begin{bmatrix} a & 0 & b & 0 \\ 0 & a & 0 & b \\ c & 0 & d & 0 \\ 0 & c & 0 & d \end{bmatrix} : a, b, c, d \in \mathbb{C} \right\}.$$

For the unitary

$$U := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \tag{11}$$

we have $U(I \otimes A)U^* = A \otimes I$ for every $A \in M_2(\mathbb{C})$. $\square$

Example 4 Try to find a unitary

$$W := \begin{bmatrix} W_1 & W_2 \\ W_3 & W_4 \end{bmatrix}$$

such that the subalgebra

$$W\begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}W^* \qquad (A \in M_2(\mathbb{C}))$$

is complementary to $I \otimes M_2(\mathbb{C})$. Assume that $\mathrm{Tr}\, B = 0$. Then the orthogonality

$$W\begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}W^* \perp \begin{bmatrix} B & 0 \\ 0 & B \end{bmatrix}$$

means that

$$\mathrm{Tr}\,(W_1AW_1^* + W_2AW_2^* + W_3AW_3^* + W_4AW_4)B = 0.$$

This holds for every B if and only if

$$W_1AW_1^* + W_2AW_2^* + W_3AW_3^* + W_4AW_4$$

is a multiple of the identity. Therefore, the sufficient and necessary condition is the following:

$$W_1AW_1^* + W_2AW_2^* + W_3AW_3^* + W_4AW_4^* = (\mathrm{Tr}\, A)I \qquad (A \in M_2(\mathbb{C}). \tag{12}$$

For the unitary

$$W := \frac{1}{\sqrt{2}}\begin{bmatrix} I & \sigma_3 \\ \sigma_1 & \mathrm{i}\sigma_2 \end{bmatrix} \tag{13}$$

the condition holds. (σ_i's are the Pauli matrices.) One computes that

$$W(I\otimes\sigma_1)W^* = \sigma_1 \otimes I, \quad W(I\otimes\sigma_2)W^* = \sigma_2\otimes\sigma_3, \quad W(I\otimes\sigma_3)W^* = \sigma_3\otimes\sigma_3.$$

We obtained an algebra determined by a Pauli triplet consisting elementary tensors of Pauli matrices. □

The previous example can be generalized.

Theorem 4 *Let $W = \sum_{ij=1}^n E_{ij}\otimes W_{ij} \in M_n(\mathbb{C})\otimes M_m(\mathbb{C})$ be a unitary, where E_{ij} are the matrix units in $M_n(\mathbb{C})$ and $W_{ij} \in M_m(\mathbb{C})$. The subalgebra $W(\mathbb{C}I \otimes M_m(\mathbb{C}))W^*$ is complementary to $\mathbb{C}I\otimes M_m(\mathbb{C})$ if and only if*

$$\frac{m}{n}\sum_{i,j=1}^n |W_{ij}\rangle\langle W_{ij}| = I.$$

When $n = m$ this condition means that $\{W_{ij} : 1 \le i, j \le n\}$ is an orthonormal basis in $M_n(\mathbb{C})$ (with respect to the inner product $\langle A, B\rangle = Tr\, A^*B$).

Proof: Assume that $A, B \in M_m(\mathbb{C})$ and $\mathrm{Tr}\, B = 0$. Then the condition

$$W(I \otimes A^*)W^* \perp (I \otimes B)$$

is equivalently written as

$$\mathrm{Tr}\, W(I \otimes A)W^*(I \otimes B) = \sum_{i,j=1}^{n} \mathrm{Tr}\, W_{ij} A W_{ij}^* B = 0.$$

Putting $B - (\mathrm{Tr}\, B)I_m/m$ in place of B, we get

$$\sum_{i,j=1}^{n} \mathrm{Tr}\, W_{ij} A W_{ij}^* B = \frac{1}{m} \mathrm{Tr}\, B \sum_{i,j=1}^{n} \mathrm{Tr}\, W_{ij} A W_{ij}^* \,.$$

for every $B \in M_m(\mathbb{C})$. Since W is a unitary, $\sum_{i=1}^n W_{ij}^* W_{ij} = I$, and we arrive at the relation

$$\sum_{i,j=1}^{n} \mathrm{Tr}\, W_{ij} A W_{ij}^* B = \frac{n}{m} \mathrm{Tr}\, A \mathrm{Tr}\, B \tag{14}$$

We can transform this into another equivalent condition in terms of the left multiplication and right multiplication operators. For $A, B \in M_m(\mathbb{C})$, the operator R_A is the right multiplication by A and L_B is the left multiplication by B: $R_A, L_B : M_m(\mathbb{C}) \to M_m(\mathbb{C})$, $R_B X = XB$, $L_A X = AX$. Equivalently, $L_A |e\rangle\langle f| = |Ae\rangle\langle f|$ and $R_B |e\rangle\langle f| = |e\rangle\langle B^* f|$.

The equivalent form of (14) is the equation

$$\frac{m}{n} \sum_{i,j=1}^{n} \langle W_{ij}, R_A L_B W_{ij} \rangle = \mathrm{Tr}\, A \,\mathrm{Tr}\, B = \mathrm{Tr}\, R_A L_B$$

for every $A, B \in M_m(\mathbb{C})$. Since the operators $R_A L_B$ linearly span the space of all linear operators on $M_m(\mathbb{C})$,

$$\frac{m}{n} \sum_{i,j=1}^{n} \mathrm{Tr}\, |W_{ij}\rangle\langle W_{ij}| X = \frac{m}{n} \sum_{i,j=1}^{n} \langle W_{ij}, X W_{ij} \rangle = \mathrm{Tr}\, X$$

for every (super)operator $X : M_m(\mathbb{C}) \to M_m(\mathbb{C})$. So we conclude

$$\frac{m}{n} \sum_{i,j=1}^{n} |W_{ij}\rangle\langle W_{ij}| = I,$$

where I is the identity acting on the space $M_m(\mathbb{C})$. □

Although the previous theorem is formulated for a tensor product, it covers the general case. If $\mathcal{A}_1$ is a subalgebra of $\mathcal{A}$, $\mathcal{A}_1 \simeq M_n(\mathbb{C})$ and $\mathcal{A} \simeq M_p(\mathbb{C})$, then $m := p/n$ is an

integer and $\mathcal{A} \simeq M_n(\mathbb{C}) \otimes M_m(\mathbb{C})$. (The subalgebra $M_m(\mathbb{C})$ is the relative commutant of $\mathcal{A}_1$.) Let us call the unitary satisfying the condition in the previous theorem as a **useful unitary**.

In the rest of the paper we work in the situation $m = n$ and we denote the set of all $n^2 \times n^2$ useful unitaries by $\mathcal{M}(n^2)$. To construct k pairwise complementary subalgebras we need k unitaries $W_1, W_2, \dots, W_k \in \mathcal{M}(n^2)$ such that $W_1 = I$ and $W_i W_j^*$ is a useful unitary if $i > j$.

Since $\langle A, WBW^* \rangle = \langle W^*AW, B \rangle$, we have $W \in \mathcal{M}(n^2)$ if and only if $W^* \in \mathcal{M}(n^2)$. This can be seen also from the condition of Theorem 4.

Question 3 Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be subalgebras of $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ such that they isomorphic to $M_n(\mathbb{C})$. Set

$$d := \sup\{\tau(P_1 P_2) : P_i \text{ is a minimal projection in } \mathcal{A}_i\}.$$

Then $d \le 1/n$. Assume that $1/n - d > 0$. Can we give a lower bound for

$$S(\varphi|\mathcal{A}_1) + S(\varphi|\mathcal{A}_2)$$

as an analogue of the uncertainty relation in Theorem 1?

Example 5 Now we generalize Example 4. We want to construct a unitary $W := \sum_{ij} E_{ij} \otimes W_{ij}$ such that $n^{-1/2} W_{ij}$ form an orthonormal basis with respect to (8).

Let X and Y be the $n \times n$ unitaries from Example 1, and let (c_{ij}) be a unitary such that $n|c_{ij}|^2 = 1$. Set

$$W_{ij} := c_{ij} X^i Z^j. \tag{15}$$

Then

$$\sum_j W_{ij}(W_{kj})^* = \sum_j c_{ij}\overline{c}_{kj} X^{i-k} = \delta_{jk} I$$

and W is a unitary. Moreover, $\mathrm{Tr}\, W_{ij}^* W_{ij} = |c_{ij}|^2 \mathrm{Tr}\, I = 1$.

In the case of $n = 2$, $X = \sigma_1$ and $Z = \sigma_3$. Similarly to (13) we have the useful unitary

$$W := \frac{1}{\sqrt{2}} \begin{bmatrix} -\mathrm{i}\sigma_2 & \sigma_1 \\ \sigma_3 & I \end{bmatrix}. \tag{16}$$

□

Since we have a unitary W in $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ such that it satisfies the condition of Theorem 4, we obtain examples of complementary subalgebras.

Example 6 Let $\mathcal{A}$ be the algebra generated by the operators a_1, a_1^*, a_2, a_2^* satisfying the **canonical anticommutation relations**:

$$\{a_1, a_1^*\} = \{a_2, a_2^*\} = I, \{a_1, a_1\} = \{a_1, a_2\} = \{a_1, a_2^*\} = \{a_2, a_2\} = 0,$$

where $\{A,B\} := AB + BA$. Let $\mathcal{A}_1$ be the subalgebra generated a_1 and $\mathcal{A}_2$ be the subalgebra generated a_2. Then $\mathcal{A}_1$ and $\mathcal{A}_2$ are complementary. In the usual matrix representation

$$a_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad a_2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

therefore

$$\mathcal{A}_1 = \left\{ \begin{bmatrix} a & 0 & b & 0 \\ 0 & a & 0 & b \\ c & 0 & d & 0 \\ 0 & c & 0 & d \end{bmatrix} \right\}, \quad \mathcal{A}_2 = \left\{ \begin{bmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & -b \\ 0 & 0 & -c & d \end{bmatrix} \right\}.$$

The unitary sending $\mathcal{A}_1$ to $\mathcal{A}_2$ is

$$V := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

which is similar to U in (11). The block matrix entries of V form obviously a basis, so Theorem 4 gives the complementarity.

More generally, consider the algebra $\mathcal{A}$ generated by the operators $\{a_i : 1 \le i \le n\}$ satisfying the relations

$$\begin{aligned} a_i a_j + a_j a_i &= 0 \\ a_i a_j^* + a_j^* a_i &= \delta(i,j) \end{aligned}$$

for $1 \le i, j \le n$. It is well-known that $\mathcal{A}$ is isomorphic to the algebra of $2^n \times 2^n$ matrices. Let $\{J_1, J_2\}$ be a partition of the set $\{1, 2, \dots, n\}$ and let $\mathcal{A}_j \subset \mathcal{A}$ be the subalgebra generated by $\{a_i : i \in J_j\}$, $j = 1, 2$. Since

$$\tau(ab) = \tau(a)\tau(b) \tag{17}$$

holds for every $a \in \mathcal{A}_1$ and $b \in \mathcal{A}_2$, the subalgebras $\mathcal{A}_1$ and $\mathcal{A}_2$ are complementary. (See [2, 5].) $\square$

Assume that $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_m$ are complementary subalgebras of $M_n(\mathbb{C}) \otimes M_n(\mathbb{C})$ and each of them is isomorphic to $M_n(\mathbb{C})$. Since the dimension of $\mathcal{A}_a \ominus \mathbb{C}I$ is $n^2 - 1$, the inequality $n^4 - 1 \ge m(n^2 - 1)$ holds. This implies that $m \le n^2 + 1$. This trivial upper bound is 5 for $n = 2$. However, the maximum number of complementary subalgebras is 4. This will be discussed in the next section.

5 Two qubits

We try to find a unitary W again such that the subalgebra

$$W \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix} W^* \qquad (A \in M_2(\mathbb{C}))$$

is complementary to $\mathbb{C}I \otimes M_2(\mathbb{C})$. The approach of the paper [21] is followed here. We may assume that W has the **Cartan decomposition**

$$W = (L_1 \otimes L_2)N(L_3 \otimes L_4)\,,$$

where L_1, L_2, L_3 and L_4 are 2×2 unitaries and

$$N = \exp(\alpha \mathrm{i}\, \sigma_1 \otimes \sigma_1) \exp(\beta \mathrm{i}\, \sigma_2 \otimes \sigma_2) \exp(\gamma \mathrm{i}\, \sigma_3 \otimes \sigma_3) \tag{18}$$

is a 4×4 unitary in a special form, see equation (11) in [27] or [10]. The subalgebra

$$W(\mathbb{C}I \otimes M_2(\mathbb{C}))W^*$$

does not depend on L_3 and L_4, therefore we may assume that $L_3 = L_4 = I$.

The orthogonality of $\mathbb{C}I \otimes M_2(\mathbb{C})$ and $W(\mathbb{C}I \otimes M_2(\mathbb{C}))W^*$ does not depend on L_1 and L_2. Therefore, the equations

$$\mathrm{Tr}\, N(I \otimes \sigma_i)N^*(I \otimes \sigma_j) = 0$$

should be satisfied, $1 \le i, j \le 3$. We know from Theorem 4 such that these conditions are equivalent to the property that the matrix elements of N form a basis.

A simple computation gives that

$$N = \sum_{i=0}^{3} c_i\, \sigma_i \otimes \sigma_i = \begin{bmatrix} c_0 + c_3 & 0 & 0 & c_1 - c_2 \\ 0 & c_0 - c_3 & c_1 + c_2 & 0 \\ 0 & c_1 + c_2 & c_0 - c_3 & 0 \\ c_1 - c_2 & 0 & 0 & c_0 + c_3 \end{bmatrix},$$

where

$$\begin{aligned} c_0 &= \cos\alpha\, \cos\beta \cos\gamma + \mathrm{i} \sin\alpha\, \sin\beta\, \sin\gamma\,, \\ c_1 &= \cos\alpha\, \sin\beta \sin\gamma + \mathrm{i} \sin\alpha\, \cos\beta\, \cos\gamma\,, \\ c_2 &= \sin\alpha\, \cos\beta \sin\gamma + \mathrm{i} \cos\alpha\, \sin\beta\, \cos\gamma\,, \\ c_3 &= \sin\alpha\, \sin\beta \cos\gamma + \mathrm{i} \cos\alpha\, \cos\beta\, \sin\gamma\,. \end{aligned}$$

From the condition that the 2×2 blocks form a basis (see Theorem 4), we deduce the equations

$$|c_0|^2 = |c_1|^2 = |c_2|^2 = |c_3|^2 = \frac{1}{4}$$

and arrive at the following solution. Two of the values of $\cos^2\alpha, \cos^2\beta$ and $\cos^2\gamma$ equal $1/2$ and the third one may be arbitrary. Let $\mathcal{N}$ be the set of all matrices such that the parameters α, β and γ satisfy the above condition, in other words two of the three values are of the form $\pi/4 + k\pi/2$. (k is an integer.) Let

$$\mathcal{N}_1 := \{N \in \mathcal{N} : \alpha \text{ is arbitrary, } \beta = \pi/4 + k_1\pi/2, \text{ and } \gamma = \pi/4 + k_2\pi/2\} \tag{19}$$

and define $\mathcal{N}_2$ and $\mathcal{N}_3$ similarly. ($\mathcal{N} = \mathcal{N}_1 \cup \mathcal{N}_2 \cup \mathcal{N}_3$.)

The conclusion of the above argument can be formulated as follows.

Theorem 5 *$W \in \mathcal{M}(4)$ if and only if $W = (L_1 \otimes L_2)N(L_3 \otimes L_4)$, where L_i are 2×2 unitaries ($1 \le i \le 4$) and $N \in \mathcal{N}$.*

It follows that $W \in \mathcal{M}(4)$ if and only if $(U_1 \otimes U_2)W \in \mathcal{M}(4)$ for some (or all) unitaries U_1 and U_2. Note that this fact can be deduced also from Theorem 4.

Example 7 A simple example for a unitary N_3 from $\mathcal{N}_3$ is

$$N_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & \mathrm{i} & 0 \\ 0 & \mathrm{i} & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

which corresponds to $\alpha = \beta = \pi/4$ and $\gamma = 0$. One can check that

$$\begin{aligned} N_3(I \otimes \sigma_1)N_3^* &= \sigma_2 \otimes \sigma_3, \\ N_3(I \otimes \sigma_2)N_3^* &= -\sigma_1 \otimes \sigma_3, \\ N_3(I \otimes \sigma_3)N_3^* &= \sigma_3 \otimes I\,. \end{aligned}$$

$\square$

A part of the example is true more generally [25]:

Lemma 1 *If $N_i \in \mathcal{N}_i$, then $N_i(I \otimes \sigma_i)N_i^*$ equals $\sigma_i \otimes I$ up to a sign for $1 \le i \le 3$.*

It is useful to know that for $N_1 \in \mathcal{N}_1$, see (19), the subalgebra $N_1(\mathbb{C}I \otimes M_2(\mathbb{C}))N_1^*$ does not depend on the integers k_1 and k_2. Therefore, it is often convenient to assume that $k_1 = k_2 = 0$. Similar remarks hold for $\mathcal{N}_2$ and $\mathcal{N}_3$ [25].

Theorem 6 *Let $\mathcal{A}^0 \equiv \mathbb{C}I \otimes M_2(\mathbb{C})$ and $\mathcal{B} \equiv M_2(\mathbb{C}) \otimes \mathbb{C}I$. Assume that the subalgebra $\mathcal{A}^1 \subset M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ is isomorphic to $M_2(\mathbb{C})$ and complementary to $\mathcal{A}^0$. Then the intersection of $\mathcal{A}^1$ and $\mathcal{B}$ is not trivial.*

Proof: There is a unitary $W = (L_1 \otimes L_2)N$ such that $\mathcal{A}^1 = W\mathcal{A}^0W^*$, L_1, L_2 are 2×2 unitaries and $N \in \mathcal{M}(4)$. Assume that $N \in \mathcal{N}_i$. Then

$$(L_1 \otimes L_2)N(I \otimes \sigma_i)N^*(L_1^* \otimes L_2^*) = \pm L_1\sigma_i L_1^* \otimes I$$

is in the intersection of $\mathcal{A}^1$ and $\mathcal{B}$ and $L_1\sigma_i L_1^*$ cannot be a constant multiple of I (since its spectrum is $\{1, -1\}$). $\square$

This theorem implies that $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ cannot contain 5 subalgebras which are pairwise complementary and isomorphic to $M_2(\mathbb{C})$. The question about the existence of 5 such subalgebras was raised in [19] and the answer was given first in [21]. The proof presented here is slightly different.

Example 8 The 4×4 matrices

$$C=\begin{bmatrix} a & 0 & 0 & b\\ 0 & c & d & 0\\ 0 & d & c & 0\\ b & 0 & 0 & a \end{bmatrix}$$

form a commutative algebra $\mathcal{C}$ isomorphic to $\mathbb{C}^4$. Concretely, the isomorphism κ maps the above matrix into

$$\kappa(c)=(a+b,a-b,c+d,c-d)\,.$$

The spectral decomposition of C is

$$C=(a+b)P_+ +(a-b)P_- +(c+d)Q_+ +(c-d)Q_-\,,$$

where

$$P_\pm=\frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & \pm 1\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ \pm 1 & 0 & 0 & 1 \end{bmatrix},\quad Q_\pm=\frac{1}{2}\begin{bmatrix} 0 & 0 & 0 & 0\\ 0 & 1 & \pm 1 & 0\\ 0 & \pm 1 & 1 & 0\\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Note that the projections $P_\pm$ and $Q_\pm$ correspond to the **Bell basis**.

Let $E_\mathcal{C}$ be the τ-preserving conditional expectation onto the subalgebra $\mathcal{C}$. This has the form

$$E_\mathcal{C}\Big(\sum_{ij} c_{ij}\,\sigma_i\otimes\sigma_j\Big)=\sum_i c_{ii}\,\sigma_i\otimes\sigma_i\,. \tag{20}$$

It follows that

$$E_\mathcal{C}(I\otimes A)=E_\mathcal{C}(A\otimes I)=\tau(A)\,I. \tag{21}$$

□

Theorem 7 *If $M\in\mathcal{C}$ is a unitary, then the subalgebras $M(\mathbb{C}I\otimes M_2(\mathbb{C}))M^*$ and $\mathcal{C}$ are complementary. In particular, $\mathcal{C}$ is complementary to $\mathbb{C}I\otimes M_2(\mathbb{C})$ and $M_2(\mathbb{C})\otimes\mathbb{C}I$.*

Proof: Assume that $A\in M_2(\mathbb{C})$ is traceless and $C\in\mathcal{C}$. We have to show that

$$\mathrm{Tr}\,C^*M(I\otimes A)M^*=0.$$

This follows from (21):

$$\begin{aligned}\mathrm{Tr}\,C^*M(I\otimes A)M^* &= \mathrm{Tr}\,M^*C^*M(I\otimes A)=\mathrm{Tr}\,E_\mathcal{C}(M^*C^*M(I\otimes A))\\ &= \mathrm{Tr}\,M^*C^*ME_\mathcal{C}(I\otimes A)=\tau(A)\mathrm{Tr}\,M^*C^*M=0.\end{aligned}$$

□

The theorem tells us that a measurement corresponding to the Bell basis is complementary to any local measurement of the two-qubit-system.

The algebra $M_2(\mathbb{C}) \otimes M_2(\mathbb{C})$ can be decomposed to complementary subalgebras. Together with the identity, each of the following triplets linearly spans a subalgebra $\mathcal{A}_j$ isomorphic to $M_2(\mathbb{C})$ $(1 \le j \le 4)$.

$$\begin{array}{l}\{\sigma_0 \otimes \sigma_1,\ \sigma_1 \otimes \sigma_3,\ \sigma_1 \otimes \sigma_2\} \\ \{\sigma_3 \otimes \sigma_1,\ \sigma_1 \otimes \sigma_1,\ \sigma_2 \otimes \sigma_0\} \\ \{\sigma_1 \otimes \sigma_0,\ \sigma_2 \otimes \sigma_2,\ \sigma_3 \otimes \sigma_2\} \\ \{\sigma_0 \otimes \sigma_2,\ \sigma_2 \otimes \sigma_3,\ \sigma_2 \otimes \sigma_1\}\,.\end{array}$$

The orthogonal complement spanned by $\{\sigma_0 \otimes \sigma_3, \sigma_3 \otimes \sigma_0, \sigma_3 \otimes \sigma_3\}$ is a commutative subalgebra.

Acknowledgement: The author thanks to Paul Busch, Domenico D'Alessandro, Patrick Hayden, Pekka Lahti, Milán Mosonyi and András Szántó for discussions on related subjects.

References

[1] L. Accardi, Some trends and problems in quantum probability, in *Quantum probability and applications to the quantum theory of irreversible processes*, eds. L. Accardi, A. Frigerio and V. Gorini, Lecture Notes in Math. **1055**, pp. 1–19. Springer, 1984.

[2] H. Araki and H. Moriya, Equilibrium statistical mechanics of fermion lattice systemsm Rev. Math. Phys. **15**, 93–198, 2003.

[3] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury and F. Vatan, A new proof for the existence of mutually unbiased bases, Algoritmica **34**, 512–528, 2002 and arXiv:quant-ph/0103162.

[4] P.O Boykin, M. Sitharam, P.H. Tiep and P. Wocjan, Mutually unbiased bases and orthogonal decompositions of Lie algebras, arXiv:quant-ph/0506089, 2005.

[5] O. Bratteli and D.W. Robinson, *Operator algebras and quantum statistical mechanics II*, Springer, 1981.

[6] D. Bruss, Optimal eavesdropping in quantum cryptography with six states. Physical Review Letters, **81**, 3018–3021, 1998.

[7] P. Busch, P.J. Lahti and P. Mittelstaedt, *The Quantum Theory of Measurement*, Lecture Notes in Physics m2, Springer, 1991.

[8] P. Busch and P.J. Lahti, The complementarity of quantum observables: theory and experiment, Rivista del Nuovo Cimento **18**, 1–27, 1995.

[9] P. Busch and C.R. Shilladay, Complementarity and uncertainty in Mach-Zehnder interferometry and beyond, quant-ph/0609048.

[10] D. D'Alessandro and F. Albertini, Quantum symmetries and Cartan decompositions in arbitrary dimensions, quant-ph/0504044, 2005.

[11] M. Florig and S.J. Summers, On the statistical independence of algebras of observables, J. Math. Phys. **38**, 1318-1328, 1997.

[12] I. D. Ivanovic, Geometrical description of quantum state determination, J. Physics A**14**, 3241–3245, 1981.

[13] G. Kimura, H. Tanaka and M. Ozawa, Solution to the Mean King's problem with mutually unbiased bases for arbitrary levels, Phys. Rev. A **73**, 050301(R), 2006.

[14] K. Kraus, Complementarity and uncertainty relations, Phys. Rev. D. **35**, 3070-3075, 1987.

[15] M. Krishna and K R Parthasarathy, An entropic uncertainty principle for quantum measurements, Sankhya Indian J. Statistics **64**, 842–851, 2002. quant-ph/0110025.

[16] H. Maasen and I. Uffink, Generalized entropic uncertainty relations, Phys. Rev. Lett. **60**(1988), 1103–1106.

[17] M. Ohya and D. Petz, *Quantum Entropy and Its Use*, Springer-Verlag, Berlin, 1993, 2nd ed. 2004.

[18] K.R. Parthasarathy, On estimating the state of a finite level quantum system, Infin. Dimens. Anal. Quantum Probab. Relat. Top., **7**, 607-617. 2004.

[19] D. Petz, K.M. Hangos, A. Szántó and F. Szöllősi, State tomography for two qubits using reduced densities, J. Phys. A: Math. Gen. **39**, 10901–10907, 2006.

[20] D. Petz, K.M. Hangos, A. Magyar, Point estimation of states of finite quantum systems, arXiv:quant-ph/0610124, 2006.

[21] D. Petz and J. Kahn, Complementary reductions for two qubits, quant-ph/0608227, 2006.

[22] A.O. Pittenger and M.H. Rubin, Mutually unbiased bases, generalized spin matrices and separability, Linear Algebra Appl. **390**, 255–278, 2004.

[23] J. Sanchez, Improved bounds in the entropic uncertainty and certainty relations for complementary observables, Physics Letters A, **201**, 125–131, 1995.

[24] J. Schwinger, Unitary operator bases, Proc. Nat. Acad. Sci. U.S.A. **46**, 570–579, 1960.

[25] A. Szántó, Student report, BUTE, 2006.

[26] W. Tadej and K. Zyczkowski, A concise guide to complex Hadamard matrices, Open Syst. Inf. Dyn. **13**, 133-177 (2006) and arXiv:quant-ph/0512154.

[27] J. Zhang, J. Vala, K.B. Whaley and S. Sastry, A geometric theory of non-local two-qubit operations, Phys. Rev. A67, 042313, 2003.

[28] W.K. Wooters and B.D. Fields, Optimal state determination by mutually unbiased measurements, Annals of Physics, **191**, 363–381, 1989.